Сливкін С. С.,
слухач магістратури,
Київський інститут Національної гвардії України
(м. Київ, Україна)

Науковий керівник:
Комісарова Н. О.,
кандидат юридичних наук, доцент, доцент кафедри забезпечення державної безпеки,
Київський інститут Національної гвардії України
(м. Київ, Україна)

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ ВІЙСЬКОВИХ ФОРМУВАНЬ ЩОДО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ

Вступ. Події останніх років переконливо засвідчили, що диверсійно-розвідувальні групи (ДРГ) становлять загрозу не лише у військовому, але й у інформаційно-психологічному вимірі. Їхня діяльність не обмежується підривами інфраструктурних об’єктів чи знищенням техніки: паралельно здійснюється поширення дезінформації, чуток і панічних настроїв, що підриває довіру до органів влади та сектору безпеки.

Особливо відчутно ця проблема проявилася у період повномасштабної агресії Російської Федерації проти України. За даними Служби безпеки України, у 2022–2023 роках неодноразово фіксувалася діяльність ДРГ, яка поєднувала диверсійні акти з інформаційним супроводом у соціальних мережах та месенджерах, що створювало атмосферу нестабільності й хаосу.

Стратегія воєнної безпеки України (2021) та Стратегія національної безпеки (2020) прямо визначають інформаційний простір одним із ключових напрямів протидії гібридним загрозам.

Досвід останніх років переконує: інформаційно-психологічний компонент діяльності ДРГ може завдавати шкоди, співмірної з наслідками фізичного ураження. Саме тому протидія диверсіям має поєднувати не лише військові та правові механізми, а й заходи у сфері інформаційної безпеки та стратегічних комунікацій.

Метою цієї роботи є визначення особливостей інформаційно-психологічних дій диверсійно-розвідувальних груп та обґрунтування комплексних підходів до їх нейтралізації у системі державної безпеки України.

Сутність інформаційно-психологічних дій ДРГ. Інформаційно-психологічний вимір діяльності диверсійно-розвідувальних груп (ДРГ) є однією з ключових складових сучасної гібридної війни. На відміну від класичних

диверсій, що спрямовані на фізичне ураження інфраструктури чи військових об’єктів, інформаційні дії покликані впливати на моральний стан, поведінку та довіру населення до державних інституцій. Саме тому їхня шкода може бути співмірною з наслідками від прямих бойових дій .

Форми інформаційно-психологічних дій. По-перше, йдеться про дезінформацію та поширення фейків. За даними Служби безпеки України, у 2022–2023 роках фіксувалися випадки, коли після диверсійних атак на об’єкти енергетики ворог розгортав масштабні інформаційні кампанії у соціальних мережах, поширюючи чутки про «тривалі блекаути» чи «нездатність влади відновити контроль» .

По-друге, ДРГ активно застосовують психологічний тиск на військовослужбовців та цивільне населення. У Сумській та Чернігівській областях навесні 2022 року диверсійні групи супроводжували мінування доріг повідомленнями в локальних чатах про «оточення» і «масовані обстріли», що фактично не відповідало реальності . Такі дії підривали довіру до офіційних повідомлень Генштабу ЗСУ та створювали атмосферу хаосу.

По-третє, поширеною практикою є комбінування диверсій і інформаційних атак. Підрив мостів, складів чи адмінбудівель супроводжується масованим поширенням чуток про «великі втрати» чи «провал оборони». Як зазначає І. Руснак, асиметричність таких дій дозволяє противнику досягати значних ефектів за мінімальних ресурсів .

По-четверте, все більшого значення набувають кібердиверсії та цифровий вплив. У 2023 році СБУ неодноразово повідомляла про ліквідацію агентурних мереж, які здійснювали злом акаунтів військовослужбовців та поширювали дезінформацію від їхнього імені . У Стратегії національної безпеки України кіберпростір визначено як один із головних напрямів забезпечення безпеки держави, що свідчить про усвідомлення масштабності цієї загрози .

Характерні риси

Аналіз досвіду війни Росії проти України показує кілька ключових ознак інформаційно-психологічних дій ДРГ:

синхронізація з фізичними диверсіями (будь-яка атака супроводжується інформаційним “підсиленням”);

адаптивність та використання локальних каналів (місцеві пабліки, групи у месенджерах);

інтеграція з агентурними мережами (колаборанти забезпечують інформаційну підтримку);

маскування під цивільні джерела для підвищення довіри аудиторії .

Приклади з російсько-української війни:

Київщина (березень 2022 р.): затримані ДРГ у Бучанському та Ірпінському районах мали при собі засоби супутникового зв’язку та інструкції щодо поширення панічних повідомлень у соцмережах .

Харківщина (осінь 2022 р.): під час контрнаступу противник залишав мобільні групи, які здійснювали підриви складів і одночасно поширювали дезінформацію про «масовий відступ ЗСУ» .

Енергетична інфраструктура (2023 р.): після атак на об'єкти енергетики бот-мережі поширювали повідомлення про «відсутність світла на кілька місяців». Ці інформаційні атаки були заблоковані СБУ у рамках кібероперацій.

Канали та методи інформаційного впливу ДРГ. Інформаційно-психологічні дії диверсійно-розвідувальних груп здійснюються через різноманітні канали комунікації, що дозволяє противнику охоплювати як військових, так і цивільне населення. Вибір методів залежить від конкретної мети: посіяти паніку, підважити довіру до влади чи створити умови для успішних диверсій.

Соціальні мережі та месенджери. Найбільш поширеним каналом впливу є соціальні мережі (Facebook, Instagram, TikTok) та месенджери (Telegram, Viber, WhatsApp). Через них поширюються фейкові повідомлення про «оточення українських військ» чи «масовані втрати серед командування». За даними Freedom House, саме Telegram у 2022–2023 роках став головним майданчиком для координації інформаційних атак проти України. Додатково, виявлені СБУ бот-мережі після ракетних ударів по енергетиці поширювали панічні меседжі про «відсутність світла на місяці».

Кібератаки та злом акаунтів. ДРГ та пов'язані з ними хакерські угруповання активно застосовують методи цифрових диверсій. Institute of Mass Information (IMI) фіксував випадки, коли зламані акаунти українських журналістів і військових використовувалися для поширення дезінформації. Подібні атаки дозволяють ворогу легітимізувати неправдиві повідомлення, оскільки вони надходять з «довірених» джерел. The Times у 2023 році повідомляла про систематичні злами акаунтів у соцмережах з подальшим розповсюдженням панічних постів.

Фейкові новинні ресурси та псевдо-медіа. Окремим інструментом стали спеціально створені інформаційні сайти й Telegram-канали, які маскуються під регіональні ЗМІ. VoxUkraine у своєму дослідженні показало, що такі «медіа» активно використовуються для поширення чуток після диверсій на місцевому рівні, наприклад, у Харківській та Сумській областях. Їхня діяльність підсилюється крос-постингом у реальні новинні спільноти.

Використання психологічних тригерів. У повідомленнях ДРГ домінують теми, що торкаються базових страхів населення: втрати рідних, брак ресурсів, зрада з боку командування. Як підкреслює NATO StratCom, саме експлуатація емоційної складової є головним механізмом успіху інформаційних атак. Дослідження Д. Кілкаллена підтверджує, що навіть невелика група може посіяти хаос, якщо зуміє правильно підібрати наратив для цільової аудиторії.

Комбінування каналів. Найбільшої ефективності досягають ті інформаційні операції, які поєднують різні канали одночасно. Прикладом є операції під час боїв на Київщині у березні 2022 року: диверсійні дії ДРГ супроводжувалися одночасним поширенням фейків у месенджерах і появою «новин» у псевдо-медіа про «масову паніку серед населення»

Наслідки інформаційно-психологічного впливу ДРГ. Інформаційно-психологічні дії диверсійно-розвідувальних груп (ДРГ) мають значні наслідки, які проявляються на різних рівнях — від індивідуального, через суспільний, до державно-політичного. Ці наслідки можуть бути як негайними, так і кумулятивними, з довгостроковими ефектами.

Психологічні наслідки для населення та військовослужбовців

Зростання страху та тривожності серед цивільного населення. За результатами опитувань та інтерв'ю, частина людей повідомляють про підвищену нестабільність та небезпеку для життя навіть у тилових зонах, через фейки чи чутки про наступ, замінування, обстріли. Зокрема, у звіті *When Words Become Weapons: Disinformation Report for Ukraine* зазначається, що надмірна кількість неправдивої інформації негативно впливає на добробут та психічний стан людей, викликає паніку чи параноїдальні настрої.

Деморалізація серед військових. Непідтверджені повідомлення про великі втрати, зраду у командуванні чи оточення підрозділів можуть підривати бойовий дух і довіру до командування.

Соціальні та суспільні наслідки. Падіння довіри до державних інститутів. Коли інформаційні вкиди та фейки стають масовими, люди починають сумніватися у офіційній інформації. Наприклад, Gallup повідомляє, що в 2024 році спостерігається зростання серед дорослого населення України кількості тих, хто хотів би швидкого переговорного завершення війни — частково через виснаження та довіру до можливостей влади.

Ослаблення соціальної згуртованості. Інформаційні атаки, які підсилюють страх, нашу відчуження між сусідами або регіонами, можуть поділити суспільство. Фейк-новини та чутки часто мають ефект «відрізання» частини населення від правильних джерел інформації, що підсилює ізоляцію.

Політичні і стратегічні наслідки. Сприяння «втомі війни» (“war fatigue”). Населення може втратити ентузіазм підтримувати активні бойові дії, особливо коли інформаційні повідомлення акцентують на довготривалих стражданнях, зниження рівня життя, проблеми з енерго- та комунальними послугами. Як показує Gallup, саме зростаюча кількість людей в Україні прагне переговорного завершення війни через втому.

Ускладнення мобілізації та підтримки заходів держави. Коли державна політика стає об’єктом дискредитації через дезінформацію, люди менш охоче виконують заклики до співпраці — наприклад, участі в заходах оборони, волонтерстві чи слідуванні обмеженням чи інструкціям, які видають військово-цивільні адміністрації.

Підрив міжнародного іміджу. Якщо інформаційні атаки супроводжуються поширенням неправдивих або перебільшених повідомлень, це може працювати проти довіри міжнародних партнерів, донорів, журналістів, аналітиків, які можуть засумніватися у достовірності інформації — що ускладнює отримання підтримки чи ефективної співпраці.

Кумулятивні та довгострокові ефекти. Ерозія медіаграмотності. Постійне зіткнення з фейками може призвести до того, що люди просто перестануть перевіряти інформацію, ставатимуть менше критичними, що спрощує життя тим, хто поширює маніпуляції.

Тривала психологічна травма. Постійний страх, паніка, невизначеність — все це ускладнює психічне здоров'я населення, може призвести до PTSD, депресій, проблем із сном, соціальної ізоляції.

Втрата історичної та культурної довіри. Коли інформація системно спотворюється або масове маніпулювання історією стає нормою, це веде до спотвореного сприйняття подій, проблем із ідентичністю.

Протидія інформаційно-психологічним загрозам. Ефективна боротьба з інформаційно-психологічними діями ДРГ потребує поєднання правових, організаційних та технологічних інструментів.

Правові засади. Закон України *«Про національну безпеку»* (2018) та *«Про боротьбу з тероризмом»* (2003) визначають інформаційну безпеку складовою державної безпеки, але не містять чіткого алгоритму взаємодії силових структур у сфері протидії дезінформації. Стратегія воєнної безпеки України (2021) наголошує на необхідності формування цілісної системи інформаційного спротиву.

Організаційні механізми. Провідна роль належить СБУ, яка регулярно викриває агентурні мережі та бот-ферми, що поширюють паніку після диверсій. Генштаб ЗСУ забезпечує стратегічні комунікації, тоді як Міністерство культури та інформаційної політики координує протидію фейкам на цивільному рівні. RAND у своєму аналізі підкреслює важливість координації між відомствами та створення єдиного центру управління інформаційними операціями.

Технологічні рішення. Українські та міжнародні експерти відзначають потребу у розвитку систем моніторингу соцмереж та застосуванні штучного інтелекту для виявлення бот-мереж. NATO StratCom у своїх звітах пропонує моделі швидкого виявлення та маркування фейкових повідомлень як частину гібридної протидії.

Практичні заходи. У 2023 році СБУ ліквідувала кілька угруповань, які здійснювали кібератаки та поширювали дезінформацію через зламані акаунти військових. Крім того, розвивається система державних онлайн-ресурсів (*"StopFake", "Єдиний портал стратегічних комунікацій"*), що дозволяють громадянам швидко перевіряти сумнівні повідомлення.

Висновки. Проведене дослідження показало, що інформаційно-психологічний вимір діяльності диверсійно-розвідувальних груп є одним із ключових факторів сучасної гібридної війни. ДРГ не обмежуються фізичними диверсіями — їхні дії супроводжуються дезінформаційними кампаніями, поширенням фейків і провокацій, спрямованих на дестабілізацію суспільства та підрив довіри до органів влади.

Основні канали впливу включають соціальні мережі, месенджери, кібератаки та псевдо-медіа, які дозволяють швидко поширювати панічні повідомлення серед широкої аудиторії. Приклади, зафіксовані Службою безпеки

України, Генеральним штабом ЗСУ та міжнародними аналітичними центрами, підтверджують: навіть локальні диверсії можуть набувати стратегічного значення завдяки інформаційному супроводу.

Наслідки таких дій проявляються у трьох площинах: психологічній (страх, деморалізація, паніка), соціальній (падіння довіри до державних інститутів, ослаблення згуртованості) та політичній (поширення «втоми від війни», ускладнення мобілізації та міжнародної підтримки).

Ефективна протидія інформаційно-психологічним загрозам потребує комплексного підходу. На правовому рівні — це вдосконалення законодавства у сфері національної та інформаційної безпеки. На організаційному — посилення координації між СБУ, ЗСУ, Національною гвардією та цивільними структурами. На технологічному — впровадження сучасних систем моніторингу та штучного інтелекту для виявлення бот-мереж. Важливим доповненням є розвиток стратегічних комунікацій та підвищення медіаграмотності населення.

Таким чином, інформаційно-психологічний компонент діяльності ДРГ слід розглядати як системну загрозу державній безпеці. Її нейтралізація можлива лише за умови поєднання силових, правових, інформаційних та суспільно-освітніх заходів.

Список використаної літератури:

1. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII.
2. Закон України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV.
3. Кримінальний кодекс України від 05.04.2001 № 2341-III.
4. Стратегія національної безпеки України: Указ Президента України від 14.09.2020 № 392/2020.
5. Стратегія воєнної безпеки України: Указ Президента України від 25.03.2021 № 121/2021.
6. Служба безпеки України. Офіційні повідомлення про викриття диверсійно-розвідувальних груп (2022–2023 рр.). – Режим доступу: https://ssu.gov.ua.
7. Генеральний штаб Збройних Сил України. Зведення та брифінги щодо діяльності ДРГ у 2022–2023 рр. – Режим доступу: https://www.mil.gov.ua.
8. Freedom House. *Freedom on the Net 2023: Ukraine Country Report.* – Washington, 2023. – Режим доступу: https://freedomhouse.org.
9. RAND Corporation. *Ukrainian Resistance to Russian Disinformation.* – Santa Monica, 2022. – 54 p.
10. NATO StratCom COE. *Hybrid Threats and Information Operations.* – Riga, 2021. – 76 p.
11. The Guardian. *Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency.* – London, 2023. – Режим доступу: https://www.theguardian.com.

12. Gallup. *Half of Ukrainians Want Quick, Negotiated End to War.* – Washington, 2024. – Режим доступу: https://news.gallup.com.